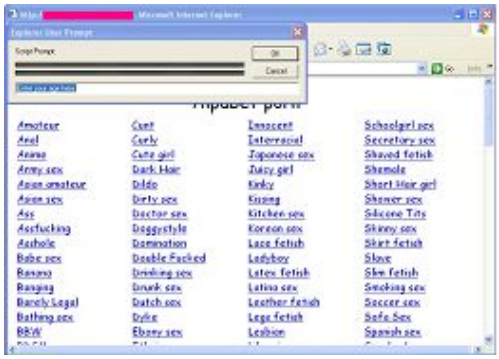
Asociación de Internautas

Primer malware que aprovecha la vulnerabilidad crítica de Explorer.

PandaLabs **ha detectado** la aparición de las primeras páginas web, de contenido para adultos, que tratan de instalar malware en el equipo aprovechando la vulnerabilidad crítica reportada recientemente para Internet Explorer, aún sin solución.

PandaLabs ha informado de la aparición de las primeras muestras de malware que utilizan la vulnerabilidad crítica de Ejecución Remota de Código de ventanas Javascript en Internet Explorer para instalarse en los equipos de los usuarios. Este aprovechamiento se lleva a cabo por medio de páginas web de contenido para adultos, que son las encargadas de atacar al ordenador e infiltrar el malware en el equipo. Dado que aún no existe solución a esta vulnerabilidad, la propagación podría ser importante en las próximas horas, por lo que se recomienda disponer de una solución antimalware actualizada, con el fin de reconocer la utilización del exploit.



El mecanismo de infección se inicia con la visita del usuario a una serie de páginas web de contenido para adultos. En ese momento, dicha página redirige el usuario a una segunda, que contiene el exploit (detectado por Panda como Exploit/BodyOnLoad) y se aprovecha de él para instalar en el equipo un primer fichero, de nombre keks.exe. Éste se instala en el equipo, y procede a descargar y ejecutar un segundo fichero all.exe. Ambos son detectados como Downloader.DLE, y tienen como principal objetivo bajar los niveles de seguridad del navegador, y ser punto de entrada de otro malware. Se da la circunstancia que en ocasiones el exploit no consigue llevar a cabo su acción de aprovechamiento; en ese caso, se registrará un error en el Explorer, y no infectará al usuario.

Si la acción de Downloader.DLE tiene éxito, instalará en el equipo varios ficheros, que resultan ser Adware/PicsPlace, un clicker que abre páginas de contenido para adultos continuamente, que generan diversas cookies maliciosas. Los clickers abren otras páginas en los equipos de los usuarios, método por el cual los creadores de malware consiguen un gran número de visitas, lo que supone un significativo lucro. Además, está programado para, periódicamente, descargarse un fichero con otras URL, con las que irá contactando, por lo que hay riesgo de entrada de nuevas variantes de malware.

Sin duda, esto es sólo el comienzo, porque una vez ha empezado a circular el exploit en manos de quienes dirigen este tipo de webs maliciosas, es sólo cuestión de tiempo que prácticamente todas lo adopten como una posibilidad más de entrar en los equipos de los usuarios , comenta Luis Corrons, director de PandaLabs. El gran problema reside en que los sistemas, pese a estar completamente

actualizados y con todos los Service Packs al día, siguen siendo vulnerables: más que nunca, es fundamental disponer de una solución antimalware completamente actualizada si no queremos correr riesgos .

La vulnerabilidad de Ejecución Remota de Código de ventanas Javascript en Internet Explorer fue detectada por primera vez el 21 de Noviembre, y afecta a Internet Explorer en Microsoft Windows 98, Windows 98 SE, Windows Millennium Edition, Windows 2000 Service Pack 4, Windows XP Service Pack 1, y Windows XP Service Pack 2. Aún no ha sido solucionada.

PandaLabs
